CommandCenter® Secure Gateway

Raritan's CommandCenter Secure Gateway (CC-SG) provides IT organizations with integrated, secure and simplified access and control of all technology platforms at the application, operating system and BIOS level.

Feature Summary

- Secure, single sign-on to a single IP address for managing all of Raritan's Dominion® KVM-over-IP switches, Paragon II analog KVM devices and Dominion PX™ intelligent PDUs
- Single point of access and audit to physical servers (including blade systems and servers), virtual machines and VMware™ infrastructure such as the ESX server and VirtualCenter enlivenments
- Centralized, role-based policy management, including controlled access privileges
- The ability to monitor, diagnose and resolve infrastructure problems
- HTML Access Client interface, which allows the user to easily locate managed equipment in customizable views, including favorites and recently accessed nodes
- Remote access and power control using HP integrated Lights-Out (iLO), Dell® Remote Access Control (DRAC), IBM® Remote Supervisor Adaptor (RSA) and IPMI service processors, plus RDP, VNC, SSH and TELNET in-band applications
- Universal Virtual Media™ control, view only or deny access policies through Dominion KX II devices
- Consolidated audit trail, including detailed activity reports

Features	Functionality	Benefits
Support for Dominion KX II	CC-SG supports access to servers and other IT equipment connected to Dominion KX II. KX II provides virtual media and Absolute Mouse Synchronization™ technology. CC-SG provides discovery, management, upgrades and many other management capabilities of KX II devices.	CC-SG provides seamless integration of access through different Dominion products such as environments with mixed Dominion KX and Dominion KX II devices.
Support for Dominion SX	CC-SG supports access to serial devices connected to Dominion SX.	You get centralized management of multiple SX units along with other Raritan access devices.
Virtualization: Integration of VMware	CC-SG provides streamlined setup of single-sign-on access to your virtualized environment, the ability to issue virtual power commands to virtual machines and virtual hosts and a topology view with one-click connections. CC-SG integrates with VMware environments and can support features like connectivity to VirtualCenter software, ESX servers and VMotion™ functionality.	You get consolidated access, power control and auditing of both physical and virtual servers. Connectivity to virtual machines is always available even when these are moved from one virtual host to another.
Support for Access to Blade Servers Connected to Dominion KX II Devices	CC-SG supports access of blade servers connected to Raritan Dominion KX II switches. Supported blade models include most Dell, HP and IBM blade servers.	You can access all connected nodes from a single client, including blade servers, non-blades, IP tools, service processors, PDU's, virtualized systems and devices connected to Raritan's KVM solutions.

Raritan.
Know more. Manage smarter.™

© 2009 Raritan Inc.

Features	Functionality	Benefits
Support for Raritan's Dominion PX	CC-SG can discover and add Dominion PX "smart" power strips located on the IP network. The CC-SG will automatically identify the firmware version, serial number and how many outlets are available on the PX. Once added to the CC-SG as a network managed device, the Dominion PX allows access to the administrative interface via a single sign-on. Additionally, Dominion PX outlets are available for configuration and association to existing CC-SG nodes (servers). Note: The option of CC-SG integration to the PX through physical connectivity to Dominion devices via power CIM or power cable is still available and supported.	You enjoy comprehensive centralized access and management. Your control of PX units can be independent of KVM or serial switches.
Access to In-Band Application and Embedded Service Processors	TELNET is supported as an in-band serial console interface. RDP, one of the most commonly used in-band console interfaces, can be used in either console or remote user modes. The RDP console allows the IT administrator to be the only RDP user on the server while the session lasts. All RDP remote console user sessions will terminate on an RDP console login. Additionally, the RDP interface can be adjusted to the desired color depth. Service accounts can be created and stored on the CC-SG with an MD5 two-way encrypted password. Service accounts can be employed on all in-band interfaces to allow for use with remote or local authentication. Changing the service account password applies to all CC-SG interfaces using that service account. Alternatively, creating specific passwords for each interface is still available.	You have the ability to connect to serial targets using TELNET protocol. You'll add flexibility by using RDP. You'll reduce the configuration time required to reflect password changes.
Robust Security	Low security profile, Linux®-based appliance architecture. A powerful policy management tool allows access and control based on a broad range of user customizable criteria, including time of day, physical location, application, operating system, department and function. Available 128-bit and 256-bit AES encryption for end-to-end node access activity through AES-enabled Dominion devices. Support for a broad range of authentication protocols, including LDAP, Active Directory®, RADIUS and TACACS+ in addition to local authentication and authorization capabilities. Ability to import user groups from Active Directory. Support for Second Factor Authentication with SecureID on RADIUS servers. IP-based access control lists (ACLs), which grant or restrict user access by IP address. Proxy mode for secure access to devices through firewalls/VPNs. Strong user password authentication, SAS 70 compliance for configurable amounts of failed login attempts and user ID lock-out parameters.	CC-SG is a powerful, hardened secure access platform that delivers peace-of-mind to IT managers who need to provide access to vital corporate resources.

© 2009 Raritan Inc.

Features	Functionality	Benefits
Neighborhood Configuration	Architecture allows a collection of up to ten CC-SG units to be deployed and work together to serve the IT infrastructure access and control needs of the enterprise.	Scalability: you can add more CC-SGs as your environment grows. Performance is enhanced through the distribution of resources across CC-SGs. Regionalization: ▶ It allows local authentication for local access. ▶ CC-SG provides around-the-clock global operations – so you can avoid failures across regions. Departmentalization/local administrative autonomy: ▶ CC-SG permits you to access network partitioning. ▶ You can segment by access tools, Raritan device type, user type, etc. You may deploy CC-SG units across different subnets.
Seamless Backup Configuration	"Cluster" configuration provides appliance redundancy through primary and secondary CC-SG deployments on different subnets and/or geographical locations.	You get instant, seamless failover if the primary unit fails.
Web Browser Access to CC-SG	CC-SG supports Web browser access to either an IP address or host name. A single sign-on via the Web browser interface is available in some applications that can accept automatic username and password entries but do not require additional entry fields like session ID. Access to the Dominion PX Web interface and Dell RAC4 administrative UI are two examples of Web browser interfaces that support single sign-on.	It provides centralized and audited access to any Web server-equipped device such as power strips, embedded service processors and Web-based proprietary IT applications.
Auditing and Audit Trail Reporting	The CC-SG administrator can sort the audit trail report based on categories. For example, the administrator can choose to view only authentication messages for remediation purposes, security messages for monitoring purposes or virtualization messages for virtual machine-related activity tracking. The administrator can choose to view only tasks, embedded- or access-related audit messages. Additionally, the administrator can use a wild card search to find specific audit messages. Node auditing requires users belonging to a group selected by the CC-SG administrator to enter free text audit information whenever accessing any interface. This information can be viewed in both the audit trail report and the node audit tab.	CC-SG permits granular audit trail sorting for specific purposes like remediation, security and debugging. It gives you the ability to capture activity reported by system users such as contractors and temporary workers.
Remote Monitoring and Capacity Planning Tools	CC-SG provides a variety of tools to monitor real-time and over-time performance of CC-SG. Once activated, these tools can capture or display information such as CPU, memory, hard disk space, etc. Using the real-time data capture tool, customers can view information in a graphic format and create e-mail alerts based on thresholds they set. With the over-time data evaluation tool, customers can see their CC-SG performance graphed over time.	CC-SG allows secure, remote monitoring tools that can be activated by customers to monitor their CC-SG hardware performance and alert them when action may be required on their part.

© 2009 Raritan Inc.

Features	Functionality	Benefits
GUI and User Experience Improvements	During its life cycle, several improvements have been introduced to the CC-SG to provide a better user experience. For example, CC-SG administrators can require acknowledgment before any power operation takes place, such as powering off a server. Additionally, the node profile was enhanced to include a tab structure that is more useful to users and includes more useful information.	The continued improvement of the CC-SG UI helps enhance the user experience for Raritan customers.
Streamlined Raritan Device Firmware Upgrade Process	The Task Manager device upgrade function includes the ability to select the number of devices to be upgraded concurrently. In addition, the user can determine a time window for the automated upgrade task. At the end of the window, no more device upgrades will be initiated by CC-SG. In order to execute a parallel upgrade, a simple select-and-move window allows the administrator to identify those devices they choose for the upgrade task. An improved Restart Device automated task has been created. The CC-SG administrator can choose multiple devices and restart them at a selected time. This is particularly useful in cases where a device restart is desired prior to or after the device upgrade. At the completion of the task, there is an Upgrade Status report generated in addition to the auto-generated e-mail alert. The Upgrade Status report provides a real-time description of the device upgrade task. The report changes based on which device is being upgraded, which was upgraded or which is yet to be upgraded.	This feature is particularly valuable in environments where a large number of Dominion devices are managed by CommandCenter, whether in a data center or distributed environment. This feature is also very useful in data centers operating 24/7 and environments where infrastructure maintenance and infrastructure downtime need to be minimized and closely monitored. The automated upgrade device is streamlined to provide a simplified yet well-controlled upgrade process for your Raritan equipment.
HP iLO2 Support	CC-SG supports single sign-on console access to HP servers equipped with iLO2 processors. In addition, CC-SG provides remote power on/off/cycle and graceful shutdown capabilities to these HP servers.	CC-SG increases productivity in environments where servers with iLO2 are deployed along with CC-SG.
Personal View Customization Using Node Groups	In addition to creating customized views by predefined categories, CC-SG 3.2 customized views can be created using predefined node groups. Group-based custom views can be created in both HTML Access Client and Java™-based admin clients. The CC-SG administrator can share custom views with all system users and, in addition, each user can create their own customized view using node groups and device groups.	For enterprise customers or large distributed IT environments where multiple groups exist, users can easily find the server or IT equipment they need to access. By easily creating custom views and modifying them on the fly, CC-SG makes the IT staff's work easier and allows them to spend more time focusing on problem resolution than searching for servers.
Virtual Media	CC-SG supports control of virtual media access policies. Three options of authorization are available for virtual media: deny, control and view only. Virtual media is available for OOB nodes connected through a virtual media CIM to a Dominion KX II device managed by the CC-SG. Virtual media can be mounted on a client system or on a remote network drive equipped with a USB connection.	This feature makes it easy to re-image (apply a new OS), boot or upgrade the device remotely.
WS-API Support	An optional WS-API is available for use with CC-SG.	This allows access of CC-SG, connected nodes and other CC-SG functions from your own customized client application.

© 2009 Raritan Inc.

Features	Functionality	Benefits
Data Import/Export	Release 4.2 includes a very comprehensive import/export capability. CSV files can be imported to help expedite the process of configuring devices, nodes, users, associations and PDUs. Import/export files include: ▶ Import and export of categories and elements ▶ Import and export of user groups and users ▶ Import and export of nodes and interfaces ▶ Import and export of devices and ports ▶ Power IQ™ import and export file	By maintaining information in a spreadsheet of IT infrastructure profiles, administrators can easily manipulate data and save it as a .csv file for importing into CC-SG, saving time. Administrators can leverage the data already in CC-SG, easily export data from CC-SG to create a master file, make any necessary changes, then return it to CC-SG or use it in other applications. Share data between CC-SG and Power IQ.

© 2009 Raritan Inc.